REMARKS

Claims 1-5, 8, 12-15, 17, 22, 9-11, 24, 25, 29-35, 49 and 50 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Rosen. Applicants respectfully traverse the rejection for at least the following reasons.

Regarding claim 1, Rosen fails to teach or suggest at least calculating in the computer of the ticket provider by use of a private key s a digital signature of third digital data D_3 as defined. Claim 1 defines, among other features, that D_3 is in respect of one or both of first digital data D_1 and D_2. D_1 is sent from a computer of the ticket provider to the computer of a prospective ticket consumer and is in respect of an occurrence for which tickets may be delivered. D_2 is sent from the computer of the ticket consumer to the computer of the ticket provider and includes an indication that a ticket is desired for the occurrence.

The office action cites col. 7, lines 30-38 and col. 6, lines 7-8 of Rosen as teaching calculation of D_3. However, col. 7, lines 30-38, instead describes an issuer signature 14 of a ticket 8, which is a digital signature formed by the ticket creator, and an issuer certificate section 16, which is a certification by a trusted third party used in conjunction with the issuer signature to verify the authenticity of the issued ticket. Particularly, the issuer certificate section 16 includes a certificate of a merchant's trusted agent (MTA) by a trusted server, and this certificate is provided during a certification process before any ticket transactions take place.

Rosen does not appear to teach or suggest that the issuer signature 14 is generated by using data corresponding to either D_1 (in respect of an occurrence for which tickets may be delivered) or D_2 (indication that a ticket is desired for the occurrence). Instead, the issuer signature 14 appears to be separate from and unrelated to identifier and component sections of the ticket.

Rosen also apparently fails to teach or suggest that the issuer certificate 16 is generated using D_1 or D_2. Instead, the issuer certificate 16 is a certification by a "Trusted Agency" to an agent, which includes both the MTA and a customer's trusted agent (CTA). This certification, as described in columns 11 and 12, initially validates a particular trusted agent, but is not specific to any occurrence. In fact, the initial certification is performed "only once, prior to distribution of the trusted agent 120 to the public" (col. 11, lines 26-27).

Additionally, col. 6, lines 7-8 fail to disclose the defined calculating, but instead describes a digital signature of an electronic object. As described in col. 5, line 59 – col. 6, line 13, the digital signature of an electronic object is for a decryption ticket, which unlocks an electronic object (such as a downloadable movie or game (see col. 4, lines 54-64)), as opposed to other types of tickets, such as event tickets. The generation of the digital signature appears based on the electronic object itself (which may be encrypted using a random number from the seller, see col. 18, line 66 – col. 19, line 11).

Thus, Rosen does not appear to teach or suggest that the digital signature is generated in respect of either D_1 or D_2. For at least these reasons, Applicants respectfully submit that claim 1 is allowable over the references of record, including Rosen.

Applicants further submit that claims 2-5 are allowable for at least the stated reasons as applied to claim 1, and for at least the reason that Rosen fails to teach or suggest features of claim 2. For example, Rosen fails to teach or suggest that D_2 includes a one-way function hash(R) of a number R which number R is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider.

The feature of R being uniquely known to the consumer, for example, allows a ticket purchaser to be anonymous when used, for example, in conjunction with an anonymous payment scheme. The purchaser knows R. The uniquely known R can then be used at ticket verification. For example, when reading into a computer of a ticket taker, the reading of Sign (s, I | | hash (R)), as further defined in claim 2, may allow the ticket taker to check if the ticket has been already used (i.e., it already knows R) and reject the ticket, or to state that the ticket is good, at which point the ticket bearer produces R (is read into computer of ticket taker), which consummates the acceptance process. Rosen, by contrast, does not appear to teach or suggest such a method to permit purchasers to remain anonymous.

The office action cites col. 11, line 67 as showing this feature, but this cited portion instead refers to certification processes between, respectively, a trusted server and a trusted agent (which agent may be the CTA or MTA), and between a primary trusted server and the trusted server. Neither process takes place between a seller and a buyer.

Also, while a hash function is disclosed in these certification processes, the hash function is used to create and check a digital signature calculated by the primary trusted server (in the first certification $\sigma_{PTS}(X)$ (col. 11, lines 62-67)) and by the trusted server (in the

second certification $\sigma_{TS}(Y)$ (col. 12, lines 1-14)). The arguments X and Y are based on information sent from the trusted agent (in the first certification) and from the trusted server (in the second certification) (col. 11, lines 17-50), and thus are known to the computer of the provider of the respective certificates, as opposed to claim 2, which defines that the number R is uniquely known to a computer of a ticket consumer.

Further, these certifications are one-time processes (though recertification may occur periodically), and they are performed prior to, and separate from, distribution of the agents for particular occurrences (col. 11, lines 26-27). Thus, the hash functions described in Rosen are not based on information that a ticket is desired for an occurrence, as D_2 is defined in independent claim 1. Additionally, the digital signatures E_{PTS} and E_{TS} do not include information I concerning an event for which the ticket is had, as defined in claim 2. Claims 3-5 inherit the features of claim 2, and their rejection is separately traversed.

Regarding claim 8, Rosen fails to teach or suggest at least calculating in the computer of a ticket consumer a number R, then second calculating in the computer of the ticket consumer a one-way function of the number R as hash(R) as defined. Further, Rosen does not teach calculating a digital signature of hash(R) appended to information I regarding the event. Instead, as explained above, the initialization/certification process of Rosen includes a hash function generated by a trusted server or primary trusted server (not a computer of a ticket consumer). Also, the certification during which the hash function is generated is not related to a particular event, and thus a digital signature E_{PTS} or E_{TS} of the hash function does not include information I relating to such an event nor a digital signature

of the same. Claims 9-23 include all of the features of claim 8, and Applicants traverse their rejection for at least the above reasons.

As to claim 24, Rosen apparently fails to teach or suggest a ticket provider's computer that digitally signs ticket order data that is transmitted from a ticket consumer's computer. Assuming that a ticket consumer's computer is described in Rosen, it would be a "customer's trusted agent" (CTA) (col. 4, lines 33-39). Even if, for the sake of argument, FIG. 23A appears to show that a CTA can send ticket order data to a ticket provider's computer, Rosen still fails to teach or suggest that this sent ticket order data is digitally signed and sent to the CTA.

Of the portions cited in the office action, col. 6, lines 7-12 merely disclose that an electronic object itself is used for a digital signature, and col. 12, lines 1-3, as explained above, relates to a certification process for a CTA or MTA, which is performed "prior to distribution of the trusted agent 120 to the public" (col. 11, lines 26-27). Thus, the cited portions do not indicate that Rosen teaches or suggests that a ticket provider's computer digitally signs ticket order data sent from a ticket consumer's computer as claimed.

For at least these reasons, Applicants traverse the rejection of claim 24. Further, regarding claim 25, Rosen fails to teach or suggest at least that the ticket consumer's computer first calculates a number R, and second calculates a one-way function of R to produce hash(R) as ticket data, as defined, and further that the ticket provider's computer calculates a digital signature in respect of the ticket data and additional information I, as also defined. Claims 26-28 inherit all of the features of claims 24 and 25, and are thus believed

also to be allowable. Regarding claim 29, Rosen fails to teach or suggest the ticket consumer's computer and ticket provider's computer for at least similar reasons as explained concerning claim 25.

Applicants have amended claim 30 to include features of claim 31. As applied to amended claim 30, Applicants respectfully traverse the rejection for at least the reason that Rosen fails to teach or suggest a digital ticket containing Sign (s, I || hash(R)) || R, where R is a random number private to the ticket consumer. The cited portions of Rosen (regarding claim 31) do not teach or suggest at least that a random number R private to the ticket consumer is used for generation of the hash function. Applicants traverse the rejection of claim 32 on similar grounds.

As to claim 33, Applicants respectfully traverse the rejection for at least the reason that Rosen fails to teach or suggest a number R having an origin in a computer of the ticket consumer and a hash function hash(R) computed in the computer of the ticket consumer and subsequently communicated to the computer of the ticket provider, as defined.

Regarding claim 34, Rosen fails to teach or suggest at least a digital ticket comprising second-type data including a signed digital representation of a particular parameter that was originally generated in sequence first by the buyer of a ticket as a non-invertible function of a random number called a "first-time-made non-invertible function", and then second by the seller of the ticket as a digital signature of the first-time-made non-invertible function", as defined.

Of the cited portions of Rosen, col. 18, lines 66-67 and col. 19, lines 1-6 refer to purchase of an electronic object and an associated decryption ticket, in which a random number generator B in merchant trusted agent B (that is, the seller of the ticket, not the buyer) creates a random key.

Further, Rosen fails to teach or suggest that the buyer attaches the selfsame random number. Instead, the electronic object is then encrypted by the MTA (the seller, particularly Symmetric Key B) with the random key generated by the MTA, and the encrypted electronic object is signed with the MTA's private key (col. 19, lines 1-12). Claims 35-37 inherit the features of claim 34, and their rejection is similarly traversed.

As to claims 49 and 50, Rosen fails to teach or suggest at least a ticket buyer computer sending at a first time a one-way transformation of a private number to a seller computer. Of the relevant cited portions of Rosen, col. 11, lines 14-67 and col. 12, lines 1-15 disclose that the hash function is performed in the trusted server and the primary trusted server for an initial certification of a trusted agent. Col. 9, lines 24-32 merely describe a transaction log within CTA's and MTA's respective computers. Accordingly, Applicants traverse the rejection of claims 49 and 50.

Claims 38-47 and 51-55 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Mengin. Applicants respectfully traverse the rejection for at least the following reasons.

Regarding claim 38, Mengin fails to teach or suggest at least a communication channel for, at a second time, sending from a ticket buyer to a ticket seller data representative

of a non-invertible transformation of a number determined by the ticket buyer only. Instead, Mengin discloses that a customer provides information such as a merchant name, inventory number, personal identification document numbers, etc. (paragraph 51). These numbers are concatenated to form a "message", and the message is digitized to form a "digimas". The "digimas" is hashed.

Mengin does not disclose that the hashed "digimas" is sent from the buyer to the seller. The cited paragraph (53) does not state which computer performs the hash function. However, paragraphs 75-77 of Mengin, describing operation flow in more detail, states that a merchant prompts an information query, and collects all of the needed information. The merchant then composes the "digimas" (paragraph 76).

Further, Mengin fails to teach or suggest the feature wherein the received digital signature of the non-invertible transformation is combined with the number to produce a digital ticket. Instead, as stated in paragraphs 54-55 cited in the office action, the merchant chooses a private key/public key pair, and the merchant composes a coded version of the "digimas" (which creates K(H("digimas")). Mengin does not appear to disclose or suggest that the argument of the non-invertible function is combined with the number used to create the "digimas" to produce the ticket. Accordingly, Applicants respectfully traverse the rejection. Claims 39-44 include all of the features of claim 38, and are similarly traversed.

Claim 45 has been amended to further include the feature wherein the 2-D bar coded indicia contains a one-way function of a number provided by a holder of a ticket. Applicants respectfully submit that at least this feature is neither taught nor suggested by

Mengin. The office action states, regarding now-cancelled claim 47, that this feature is found in paragraphs 53-55 of Mengin. However, these paragraphs refer to the "digimas", which is a digitally encoded message. The "digimas" is provided by the merchant (by encoding a message), and is not a number provided by the holder of the ticket. Accordingly, Applicants request reconsideration and withdrawal of the rejection of amended claim 45 and dependent claims 46 and 48.

As to claim 51, Mengin fails to disclose or suggest sending from the computer of the ticket seller to the computer of the ticket buyer second data accompanied by a secure first transformation of a number that is determined by the ticket buyer only and unknown to others including the ticket seller. As stated in paragraphs 51-55, a message is concatenated (by the merchant, as described above) in a prescribed, constant order and is reinterpreted digitally to form a number (the "digimas"). This number is derived by the merchant according to data provided by the customer. As the number is derived by the merchant, it would also appear to be known by the merchant. Further, the first transformation (hashing) of the number is performed by the merchant in Mengin (paragraph 55), as opposed to sending a secure first transformation from the buyer to the seller.

Additionally, Mengin fails to teach or suggest the defined storing, with the computer of the ticket buyer within a tangible portable medium of digital data storage, the number in accompaniment to a second transformation of the secure first transformation. Instead, FIG. 4 (merely showing a floppy disc) apparently provides only that a ticket can be

saved. Accordingly, Applicants respectfully traverse the rejection of claim 51 and dependent claims 52-55.

Claims 6, 7, 16, 18-21, 23, 26-28, 36, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rosen in view of Mengin. Applicants respectfully traverse the rejection for at least the reasons stated above regarding Rosen. Further, claim 48 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Mengin in view of Rosen. Applicants respectfully traverse the rejection for at least the reasons stated above regarding Mengin.

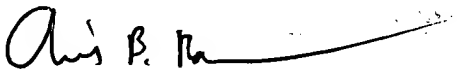
For at least the foregoing reasons, Applicants believe that this case is in condition for allowance, which is respectfully requested. The Examiner should call Applicants' attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

Customer No. 24978

May 27, 2004

By: 

Arik B. Ranson
Registration No. 43,874

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: (312) 360-0080
Facsimile: (312) 360-9315
P:\DOCS\0321\67683\535837.DOC